Sauvegardes régulières

Mis à jour le 09/01/2025

Pourquoi sauvegarder régulièrement ?

Une sauvegarde robuste et bien conçue permet de :

- **Assurer la résilience** face aux incidents (de sécurité et de production) ;
- **Restaurer** rapidement les systèmes impactés ;
- **Limiter les pertes** financières et opérationnelles.

Ainsi, disposer de sauvegardes constitue un pilier central, **notamment en cas d'incident majeur**. Elles permettent une restauration et une reconstruction du SI ainsi que le redémarrage des activités de l'entreprise.

Quels sont les points de vigilance ?

Les **données à caractère personnel,** qu'elles soient relatives aux employés ou aux clients, nécessitent des **mesures de protection renforcées pour garantir leur intégrité, leur confidentialité, leur disponibilité et leur résilience** en application du règlement général sur la protection des données (RGPD). Les dispositifs juridiques de protection et de conservation des données s'appliquent également aux dispositifs de sauvegarde.

De plus, il est nécessaire de **tester régulièrement les sauvegardes** pour vérifier **leur fiabilité**.

Ressources utiles

- Règles de sauvegarde des SI de Santé de la PGSSI-S [PDF]
- Recommandations de l'ANSSI sur les sauvegardes sécurisées [PDF]
- Recommandations de la CNIL en cas de rançongiciel [Site web]

Bonnes pratiques en matière de sauvegardes

- **Inventorier les données à sauvegarder :** Les systèmes d'information doivent être recensés et les données essentielles à la poursuite de l'activité identifiées. Il faut ainsi distinguer les **données métiers** nécessaires au fonctionnement des services (fichiers client, données manipulées par les applications, etc.) des **données techniques** nécessaires à la reconstruction du SI (sources d'installation, licences, fichiers de configuration des applications, certificats, clés, etc.). De même pour les **données de santé et de soins**.
- **Définir la fréquence des sauvegardes** : Il est recommandé de **définir le rythme des sauvegardes en fonction des risques** et de la fraicheur de données souhaitées lors d'une restauration Chaque type de sauvegarde doit avoir une fréquence dédiée. Par exemple, les sauvegardes en ligne peuvent se faire quotidiennement et les sauvegardes physiques de manière hebdomadaire).
- **Diversifier les supports de sauvegardes** : Pour plus de souplesse et de résilience, il convient de s'appuyer sur des **sauvegardes en ligne** par exemple sur des disques réseaux (SAN/NAS) ou des services Cloud qui permettent une fluidité et une agilité des sauvegardes. En revanche, elles sont exposées aux incidents et nécessitent d'avoir un réseau opérationnel pour être déployées. Il est donc nécessaire de compléter le dispositif de sauvegarde par des **sauvegardes dits « hors ligne » ou déconnectés**. Il peut par exemple s'agir d'un support physique (disque dur, serveur dédié, bandes magnétiques, …), à isoler impérativement du système d'information à l'issue de la sauvegarde.

La règle du « 3-2-1 » permet de se protéger contre des rançongiciels : 3 copies de sauvegarde, dans 2 lieux différents avec 1 copie hors ligne.